LinkedIn information used to spread banking malware in the Netherlands

By maartenvandantzigfoxit

Published: 2016-06-07 · Archived: 2026-04-05 18:10:27 UTC

Blog

June 7, 2016June 7, 2016 2 Minutes

Since early this morning (7th of June 2016, around 08:30 AM) the Fox-IT Security Operations Center started detecting a large amount of phishing e-mails containing a malicious Word document. This e-mail campaign appears to be targeting the Netherlands, using Dutch text in both the e-mail and Word document. The content of the e-mail:

```
Geachte Firstname Lastname,
Role, Company

Wij schrijven u in verband met de factuur met nummer 014321463.
De nota staat open sinds 9-jun-16. Het openstaande bedrag is 2,487.50 Euro.
Vriendelijk verzoeken wij u het openstaande bedrag te betalen.

Betaling graag zo spoedig mogelijk.

Met vriendelijke groet,

A.E. De Kuiper,
BEEREJAN HOLDING BV.
Faisantenstraat 53 Hilversum 1211 PT
Tel. +31180647000
Fax. +31294484970
```

The first name, last name, role and company name are all values that are taken from the LinkedIn page of the receiver of the phishing mail, giving the e-mail a very personalized look.

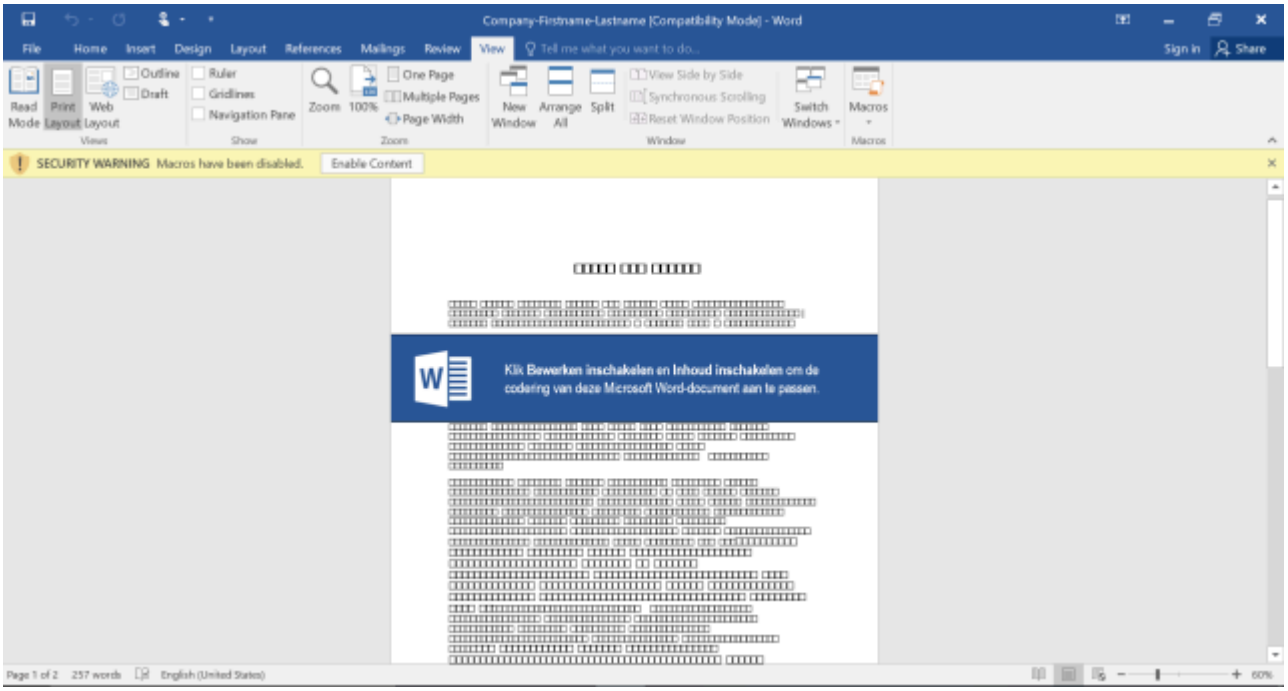
The subject of the e-mail contain the company name, with a semi-random invoice related subject. Some examples:

- **Company** : De nota is nog niet betaald
- **Company** – De nota is onbetaald gebleven
- **Company** – Uw laatste factuur wacht op betaling

At this point Fox-IT cannot directly link this phishing campaign to the recent LinkedIn database leak.

The e-mail contains a Word document with a Macro.
The name of the document is also based on personal information of the receiver:

- **Company-Firstname-Lastname.doc**



The content of the Word document appears to be scrambled, this is an attempt to trick the user into running the embedded Macro, in order to view the document.

The Macro retrieves a binary from the following (likely compromised) website:

- *ledpronto.com/app/office.bin (sha256: c1e21a06a1fa1de2998392668b6910ca2be0d5d9ecc39bd3e3a2a3ae7623400d)*

The Fox-IT InTELL team has identified the retrieved malware as the Zeus Panda banking malware. Zeus Panda, in this case, always connects to the following domain & IP using SSL:

- *skorianial.com / 107.171.187.182*

Zeus Panda is a type of banking malware based on Zeus source code, more information can be found here: https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market

The following SSL certificate is used by the Panda Zeus Command and Control server:

If you've opened the Word attachment and enabled the Macro, consider scanning your system with various anti-virus solutions.

Published June 7, 2016June 7, 2016

Post navigation

Source: https://blog.fox-it.com/2016/06/07/linkedin-information-used-to-spread-banking-malware-in-the-netherlands/